

AFFIDAVIT IN SUPPORT OF APPLICATION UNDER RULE 41 FOR SEARCH
WARRANT

I, FBI Special Agent Ryan T McGee, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is made in support of an application for a Search Warrant to search and seize evidence of a violation of 25 CFR 11.408 (Indecent Exposure) from a silver Apple iPhone XR containing SIM Card # 89148000008914428994 in a black case initially seized by Tohono O'odham Police Department ("TOPD") personnel, and later transferred to FBI Special Agent Ryan T McGee. This phone is referred to as **Target Device 1** and is further described in Attachment A of this Application (which is attached and incorporated herein for reference). Further, I submit there is probable cause to believe that the forensic extraction of **Target Device 1** contains evidence, fruits, and instrumentalities of this crime as well as the identities of persons involved, as more fully described in this search warrant and the attachments. The applied for warrant is to authorize a search of the forensic extraction of **Target Device 1** described in Attachment A for the purpose of identifying electronically stored data more particularly described in Attachment B. **Target Device 1** is currently in the possession of Federal Bureau of Investigation, secured at the Tucson Resident Agency.

2. I am an FBI Special Agent assigned to the Phoenix Division / Tucson Resident Agency. I have been a Special Agent since April 22, 2012. I completed the Basic Field Training Course at the FBI Academy in September 2012, where I received instruction in constitutional law, criminal law, and federal and civil statutes. I am a sworn investigative or law enforcement officer and am empowered by law to conduct investigations and to make arrests.

3. In September 2012, I began work as a Special Agent in the Tucson Resident Agency. I worked on International Terrorism cases for two years, Domestic Terrorism cases for eight years, and have been working Indian Country cases since January 2023. As a Special Agent, I have conducted investigations involving illicit activity and have gathered and structured evidence and facts pertaining to administrative and criminal cases. I have taken sworn statements from material witnesses and suspects. I routinely perform record checks through various law enforcement

databases to establish accuracy of information as well as gather facts relevant to cases and I have assisted fellow agents in the development of their cases.

4. Through my training and experience as a Special Agent in various types of cases, I have learned that people utilize their cell phones for many different things and including but not limited to communications, browsing the internet, scheduling, photography/videography, navigation. My experience when examining cellular phones is that you can uncover evidence that reveals or suggests who possessed or used the device, evidence of where such persons were when they possessed or used the device; evidence of who such persons were with when they possessed or used the device; and evidence of persons with whom they communicated, including all of the preceding at the time of the suspected offense(s).

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement personnel and witnesses. Since this affidavit is submitted for the limited purpose of securing a search warrant, I have not included all facts known to me regarding this investigation. I have set forth facts sufficient to establish probable cause to believe that the defendant referred to in this investigation committed Indecent Exposure.

6. In the course of conducting investigations over my years of law enforcement employment, I have interviewed persons involved with various sex crimes. I have consulted with other experienced investigators concerning the practices of sex offenders and the best methods of investigating them. In preparing this Affidavit, I have conferred with other Special Agents and law enforcement officers involved in this investigation. Furthermore, I have personal knowledge of the following facts or have learned them from the individuals mentioned herein.

7. Based on my background, training, and experience, I know that individuals who are involved in sex crimes often do the following:

- a. Use cellular telephones and laptops to arrange, coordinate, and record activities with victims and also with peers or coconspirators;
- b. Use all the communication technologies available within the particular cellular telephone and laptop, including voice messaging, texting, audio communication, direct

dial, push-to-talk, emailing, internet access, speed dial, photo and video images, in furtherance of their crimes;

c. Use multiple cellular telephones and often change cellular telephones to avoid detection by law enforcement;

e. Use cellular telephones to store and maintain contact lists containing the names, nicknames, telephone numbers, e-mail addresses and social media profile identifiers of other criminal associates and victims; communicate with victims and other criminal associates by voice, e-mail and text message, including through Apple iMessage and Face Time, as well as third-party applications such as WhatsApp, Facebook Messenger, Instagram, Snapchat, TikTok, and Signal; record, store and share with other criminal associates, including through the use of third-party applications, photographs, videos and other evidence of illicit activity.

8. The facts which establish the probable cause necessary for issuance of this order: are personally known to me; are contained in official government or business records I have reviewed; or have been told to me directly by other members of the investigative team, which includes Federal, State, or Local law enforcement officers with whom I have worked on this investigation. As this affidavit is submitted for a limited purpose, it does not contain all aspects of this investigation, but it does contain sufficient information to establish probable cause in support of a Search Warrant to search the above-mentioned phone.

9. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 25 CFR § 11.408 have been committed by VERDUGO. I further submit that there is probable cause to search the information described in Attachment A for evidence, fruits, contraband, and instrumentalities of the foregoing crime, as further described in Attachment B.

BACKGROUND ON SMARTPHONES

10. Based upon my knowledge, training, and experience, as well as information related to me by law enforcement officers and others experienced in the forensic examination of electronic communication devices, I know that certain types of cellular telephones referred to as

“smartphones” (such as **Target Device 1**) generally offer more advanced computing ability and internet connectivity than standard cellular telephones. Provided that internet access has been purchased through an electronic communication service provider for a particular smartphone, a smartphone is capable of running complete operating system software, has full access to the internet and/or electronic mail (including file attachments), is capable of text and instant messaging, can create and edit documents created with computer software, is capable of storing large amounts of data, is capable of tracking and navigating via cell towers and GPS satellites, and can be interfaced with desktop and laptop computers.

11. As described in Attachment B hereto, this affidavit seeks permission to locate not only data files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes which individual(s) used the device as well as the purpose of their use.

12. As described in Attachment B hereto, this affidavit also seeks permission to search and seize certain electronic records that might be stored within the device. Some of these electronic records might take the form of files, documents, or other data that are user generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

13. Although some of the records requested in this affidavit might be found in the form of user-generated documents (such as electronic format documents (PDF), picture (JPG), and movie files (MPx), electronic communication devices (such as **Target Device 1**) can contain other forms of electronic evidence that are not user-generated. In particular, an electronic communication device may contain records of how it has been used and/or the person(s) who utilized the electronic communication device. Based upon my knowledge, training, experience, as well as information related to me by law enforcement officers and other persons involved in the forensic examination of electronic communication devices, I know that:

- a. Data on electronic communication devices not currently associated with any file can provide evidence of a file that was once on the electronic communication device, but has since been deleted or edited, or of a deleted portion of a file;

b. Virtual memory paging systems can leave traces of information on an electronic communication device that can be used to determine what tasks and processes were recently in use;

c. Web browsers, e-mail programs, social media platforms, and chat programs store configuration information on the electronic communication devices that can reveal information such as online nicknames and passwords;

d. Operating systems can record additional information, such as the attachment of peripheral electronic devices, and the number of occasions in which the peripheral electronic devices were accessed;

e. Computer file systems can record information about the dates that files were created and the sequence in which they were created. This information may be evidence of a crime, including pre-planning or post-destruction of evidence, and indicate the existence and/or location of evidence in other areas on the electronic communication device;

f. When an electronic communication device has more than one user, files can contain information indicating the dates and times that the files were created as well as the sequence in which the files were created, and whether a particular user accessed other information close in time to the file creation dates, times, and sequences;

g. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying an electronic communication device user, and contextual evidence excluding an electronic communication device user. All of these types of evidence may indicate ownership, knowledge, and intent to commit a given offense; The foregoing type of evidence is not "data" that can be segregated, that is, this type of information cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how electronic communication devices operate and how electronic communication devices are used.

Therefore, contextual information necessary to understand the evidence to be seized, as described in Attachment B also falls within the scope of the warrant.

PROBABLE CAUSE

14. Special Agents from the FBI, and Officers from the Tohono O'odham Police Department ("TOPD") are currently investigating a series of indecent exposures and sexual harassments at the San Xavier Mission Church (SXMC). A maintenance worker at SXMC, RODOLFO VERDUGO (VERDUGO), had sexually harassed and/or exposed himself to at least two female employees. VERDUGO asked a female employee, ALLISON RENE CAMPUS (CAMPUS), how she pleases her boyfriend sexually, asked if he could see her old bathing suit pictures from beauty pageants so he could enlarge them and put them in his maintenance room, touched her leg and chest without consent, and changed his pants while CAMPUS was in the room. He also exposed himself and actively masturbated while driving another female employee, MONIQUE MORENO (MORENO), home after work.

INDECENT EXPOSURE ON 3/14/2023

15. On 3/14/2023, VERDUGO offered a fellow employee, MORENO, a ride home from SXMC. When MORENO initially opened the door to get in the vehicle, she saw a box of condoms on the seat, which made her uncomfortable, but she got in anyway. VERDUGO asked her to help him take a video for a "friend." MORENO, who was seated in the front passenger seat, took his phone and held it with her right hand across her body to record whatever VERDUGO was doing as she continued looking straight ahead. She noticed that this time VERDUGO was not taking the most direct route to her house, despite knowing where she lived. Out of her peripheral vision, MORENO noticed that VERDUGO had taken down his pants to his ankles and began masturbating, and switched hands, all while driving. Upon realizing what was happening, MORENO "went blank," froze, leaned against the passenger side door, and repeatedly asked VERDUGO to take her home. In response, VERDUGO said 'Ok. Ok. Let me pull my pants up.' VERDUGO dropped her off at her house.

16. MORENO promptly reported the incident to TOPD the same day. TOPD Sergeant Robledo #131, reached out to VERDUGO telephonically at first. According to TOPD Report #230314050, authored by Sgt Robledo:

“Verdugo admitted over the phone to exposing his penis, manipulating it and pulling his pants down, all while driving MORENO in the vehicle. He said he was making a video for his girlfriend because it was her birthday and that MORENO consented to filming it. I asked if he specifically told her what he was going to do in the video and he said yes. I asked him to tell me exactly what he told her he was going to do and he said, that he was going to make an intimate video for his girlfriend but made no mention of exposing his penis. I asked if he was very clear and if he told her that he was going to expose his penis and he insisted that he did and that he had video proof. He said he recorded their conversation prior to him exposing himself and that she gave consent.”

17. VERDUGO agreed to meet Sgt Robledo at Del Sol Casino, located at 5655 W Valencia Road, to show Sgt Robledo the proof. According to TOPD Report #230314050, authored by Sgt Robledo:

“I advised him of his *Miranda* Rights, which he waived. I explained the difference in custody / interrogation over the phone versus in person and he understood. I asked him to show me his phone and he was all to willing to show me the video. The video begins with him driving and his penis is already exposed through the fly of his pants. There is no discussion of what is about to happen or if she was ok with it. He tells her to point the phone at him and he says something about the video being for “her birthday.” He asks how the video is coming out and she says, “ok” then he unbuckles his seatbelt and pulls his pants down past his knees then re-buckles the seatbelt as he continues driving. The phone is focused on VERDUGO; MORENO’s facial expressions and body language cannot be observed. He asks her twice if she is ok and she replies that she is. He touched himself twice briefly but when he starts to manipulate himself by stroking his penis, the camera angle changes and she seems to become increasingly uncomfortable. From the open window and loud rattling of the roadway, I can tell they are traveling on Little Nogales

road and it is obvious when he turns west onto Campus drive, based on my familiarity with the roads. He slows down and pulls off the roadway and this is when she can be heard asking him to take her home. She tosses the phone onto the dashboard and Verdugo apologized repeatedly before grabbing the phone and stopping the video.”

18. Sergeant Robledo confiscated the phone from VERDUGO because it contained evidence of a crime. VERDUGO provided the unlock code for the phone, 101955. The phone was transferred to FBI custody on 3/30/2023 where it has remained in safe storage ever since.

19. At approximately 7:00pm on 3/14/2023, around the time he met with TOPD Sgt Robledo, VERDUGO texted MORENO “I’m so sorry it came to this” and “I hope you reconsider this.”

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved

by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision. Virtually all smartphones contain GPS antennae.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device, such as some tablets, used for storing data (including names, addresses, appointments, photos, or

notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card, SIM, or other removable storage media for storing data, as well as a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word- processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device or guiding its user(s).

f. Tablet: A tablet is a mobile computer very similar to a PDA, typically larger than a phone yet smaller than a notebook computer that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer or smartphone, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, messaging, and participating in Internet social networks and communication programs.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four groups of numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between

devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. Cloud Storage: Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on storage servers that are built on virtualization techniques.

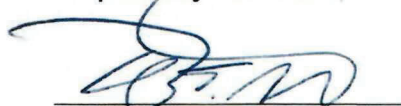
21. Based on my training, experience, and research, I know that these devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, the nature of sex crimes including Indecent Exposure, subjects sometimes memorialize their actions utilizing wireless telephones, such as **Target Device 1**. As such, examining data extracted from devices of this type frequently uncover, among other things, evidence of the crime of Indecent Exposure as well as revealing or validating particular details regarding the instant criminal conduct.

CONCLUSION

22. Based on the foregoing, I submit that there is probable cause to believe that there is evidence or property designed for use, intended for use, or used in committing violation of 25 CFR § 11.408 to search the items described in Attachment A for the items described in Attachment B and I request that the Court issue the proposed search warrant.

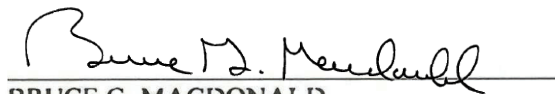
I swear, under penalty of perjury, that the foregoing is true and correct.

Respectfully submitted,



Ryan T. McGee
Special Agent
Federal Bureau of Investigation

Electronically subscribed, submitted, and sworn to telephonically on September 16th, 2024.



BRUCE G. MACDONALD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

IDENTIFICATION OF ITEM TO BE EXAMINED

The property to be searched, identified hereinafter as the **"TARGET DEVICE 1:"**

Silver Apple iPhone XR containing SIM Card # 89148000008914428994 in a black case, belonging to Rodolfo VERDUGO.

The Item is in FBI custody at the Tucson Resident Agency, located at 275 N Commerce Park Loop, Tucson, AZ 85745.

This item is logged as follows:

Item 1B1 in FBI Case # 189V-PX-3739492,

E5077003 – TCART Tucson CART Storage Area located in Tucson Evidence Control Room,

E5077071 – TCART, UNIT44, CART Storage Area located in Tucson Evidence Control Room,

Barcode E7181021.

ATTACHMENT B

DESCRIPTION OF EVIDENCE TO BE SEARCHED FOR AND SEIZED

All data on the Item described in Attachment A that relates to violations of 25 CFR § 11.408 by Rodolfo VERDUGO and other co-conspirators unknown to your affiant at this time; including:

- a. Any and all data relating to sent and received telephone calls (call history logs);
- b. Any and all data related to text messages including incoming and outgoing, forwarded, draft text messages, and third-party applications messages, with all attachments that accompany the respective text messages;
- c. Any and all data related to instant messenger and/or social networking applications including incoming, outgoing, forwarded, and draft instant messages, with all attachments that accompany the respective instant messages, and any profiles of users;
- d. Any and all photographs and videos;
- e. Any and all voicemail messages;
- f. Any and all emails;
- g. Any numbers stored for speed dial, pager numbers, address book, names, addresses, memos, notes, calendars, to do lists, electronically stored voice recordings, internet history, and/or identifying information and information uniquely identifying the cellular telephone; and
- h. Any location data, including GPS coordinates, stored on **Target Device 1**.
- i. Any and all terms/searches conducted within **Target Device 1's** internet browsers.

As used above, the term "data" includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as flash memory or other media that can store data) and any photographic form.